

1 **Amendments to the Claims:**

2 This listing of claims will replace all prior versions, and listings, of claims in the application:

3
4 1. (Currently Amended) A method of preventing piracy of a given software application
5 comprising the steps of:

6 assigning a unique identification code to each authentic copy of such software application;

7 installing the software application in a data storage element on a user's computer;

8 configuring the software application to require service data to activate at least part of its

9 functionality ~~become fully functional~~;

10 requiring a user to enter into the user's computer ~~personal~~ identifying data that identifies
11 the user;

12 requiring the user to communicate user data over a communications network ~~with~~ to a
13 remote service system, the user data being derived, at least in part, from the ~~personal~~ identifying
14 data that identifies the user, and being derived, at least in part, from the unique identification code;

15 archiving user data received from the user over the communications network in a data
16 storage element of the remote service system, said remote service system being connected to said
17 communications network and designated to receive said user data;

18 comparing received user data for each unique identification code with previously archived
19 user data corresponding to the same unique identification code to determine whether said user is
20 pirating said software application;

21 selectively transmitting service data to the user's computer from said remote service system
22 when said remote service system determines that said service data should be transmitted, said ~~user~~
23 ~~system~~ user's computer being connected to said communications network and designated to
24 stably receive said service data.

25
26 2. Canceled.

27
28 3. (Previously amended) The method as in Claim 1,

1 wherein said user data comprises the unique identification code that identifies said software
2 application installed on a data storage element of the user's computer.

3
4 4. (Currently amended) The method as in Claim 1,

5 wherein said user data includes said ~~personal~~ identifying data that identifies the user.
6

7 5. (Previously amended) The method as in Claim 1,

8 wherein said user data includes product information relating to said software application
9 installed on the data storage element of the user's computer.
10

11 6. Canceled.
12

13 7. Canceled.
14

15 8. Canceled.
16

17 9. Canceled.
18

19 10. Canceled.
20

21 11. Canceled.
22

23 12. (Currently amended) The method as in Claim 1,

24 wherein said service data [is] ~~extracted from said archived data by element for processing~~
25 ~~said service data~~ is maintained in the data storage element of the remote service system.
26

27 13. (Currently amended) The method as in Claim 12,
28

1 wherein said service data comprises at least one program code sequence that activates at
2 least part of the functionality of said software application stored on said data storage element of the
3 user's computer.

4
5 14. (Previously amended) The method as in Claim 12,

6 wherein said service data includes at least one program code sequence that results in a
7 promotional message that may be displayed to said user on the user's computer system.

8
9 15. Canceled.

10
11 16. Canceled.

12
13 17. Canceled.

14
15 18. (Previously amended) The method as in Claim 1,

16 wherein said service data is derived at least in part from said user data stored on said data
17 storage element of said remote service system.

18
19 19. (Previously amended) The method as in Claim 1,

20 wherein the step of selectively transmitting said service data is an uploading event in which
21 said service data is automatically transferred from said remote service system and storablely received
22 by the user's computer system.

23
24 20. (Previously amended) The method as in Claim 1,

25 wherein the step of selectively transmitting said service data is an uploading event in which
26 said service data is manually transferred from said remote service system and storablely received by
27 the user's computer system.

1 21. (Previously amended) The method as in Claim 1,

2 wherein the step of selectively transmitting said service data is a downloading event in
3 which said service data is made available to said user from said remote service system, and wherein
4 said user downloads said service data into the user's computer system.

5
6 22. (Currently amended) The method as in Claim 1,

7 wherein said software application includes a program code sequence that identifies said
8 software application stored on said data storage element of the user's computer system, said
9 software application additionally being responsive to a second program code sequence that
10 activates at least part of the functionality of said software application, and which is transmitted to
11 the user's computer system via said communications network.

12
13 23. (Currently Amended) A system for preventing piracy of a given software application, said
14 software application having a unique identification code associated therewith, and said software
15 application requiring service data to ~~render~~ activate at least part of the functionality of said
16 software application ~~completely functional~~, said system comprising:

17 a user computer system on which a user desires to operate the software application, said
18 user system being connected to a communications network to transmit user data and to storablely
19 receive said service data, said user data being derived at least in part from personal identifying
20 data entered by the user on the user computer system which identifies the user, and being derived at
21 least in part from said unique identification code;

22 a remote service computer system connected to said communications network to storablely
23 receive user data transmitted ~~received~~ over the communications network from the user computer
24 system said remote service computer system transmitting said service data to said user computer
25 system over said communications network when it is determined ~~said remote service computer~~
26 ~~system determines~~ that said user is not pirating said software application.

1 24. (Previously amended) The system as in Claim 23

2 wherein said remote service computer system includes a data storage element for archiving
3 user data for each unique identification code, wherein said remote service computer system
4 compares user data received from the user computer system to user data previously archived by said
5 remote service computer system relative to the same unique identification code, and wherein said
6 remote service computer system transmits said service data to said user computer system when said
7 user data received by said remote service computer system is consistent with user data previously
8 archived by said remote service computer system relative to the same unique identification code.

9

10 25. (Currently amended) The system as in Claim 23

11 wherein said service data is [is] maintained by said remote service computer system in the
12 data storage element used to archive said ~~user~~ service data.

13

14 26. (Currently amended) The system as in Claim 23

15 wherein said service data ~~is generated from said archived user data~~ consists, at least in part,
16 of an activation code sequence to activate at least part of the functionality of the software
17 application.

18

19 27. (Previously amended) The system as in Claim 23

20 wherein said service data is automatically transferred by said remote service computer
21 system and storable received by said user computer system.

22

23 28. (Previously amended) The system as in Claim 23

24 wherein said remote service computer system manually transfers said service data from said
25 remote service computer system to said user system.

26

27 29. (Currently amended) The system as in Claim 23

28

1 wherein [said] said remote service computer system makes said service data available to
2 said user from said remote service system , said user being able to download said service data into
3 said user computer system ~~for storingly receiving said service data~~ .
4

5 30. (Currently amended) The system as in Claim 23,

6 wherein said software application includes a program code sequence that identifies said
7 software application stored on said data storage element of said user system, said software
8 application additionally being responsive to a second program code sequence that activates at least
9 part of the functionality of said software application, and which is transmitted to said user system
10 via a communications network.
11

12 31. (Currently amended) A method of preventing piracy of a given software application
13 comprising the steps of:

14 assigning a unique identification code to each authentic copy of such software application;
15 installing the software application in a data storage element on a user's computer;
16 configuring the software application to require service data to ~~become fully functional~~
17 activate at least part of its functionality ;

18 requiring a user to enter into the user's computer ~~personal~~ identifying data that identifies
19 the user;

20 requiring the user to communicate user data over a communications network ~~with to~~ a
21 remote service system, the user data being derived, at least in part, from the ~~personal~~ identifying
22 data that identifies the user, and being derived, at least in part, from the unique identification code;

23 examining user data received by the remote service system from the user' computer to
24 determine whether the user is pirating the software application;

25 selectively transmitting service data to the user's computer from said remote service system
26 when said remote service system determines that the user is not pirating the software application;
27 and
28

1 storably receiving the transmitted service data within the data storage element of the user's
2 computer to ~~render the software application fully functional~~ activate at least part of the
3 functionality of the software application .
4

5 32. (Currently amended) The method recited by ~~claim~~ Claim 31 further including the step of
6 archiving user data received from users over the communications network in a data storage
7 element of the remote service system , ~~and wherein said examining step includes the step of~~
8 ~~comparing received user data for each unique identification code with previously archived~~
9 ~~user data corresponding to the same unique identification code to determine whether said~~
10 ~~user is pirating said software application~~ .
11

12 33. (New) The method recited by Claim 32,
13 wherein received user data for each unique identification code is compared with previously
14 archived user data corresponding to the same unique identification code.
15

16 34. (New) The system as recited in Claim 26,
17 wherein said service data includes at least one program code sequence that results in a
18 promotional message that may be displayed to said user on said user computer system.
19

20 35. (New) A method of preventing piracy of a given software application comprising the steps of:
21 a. assigning a unique identification code to each authentic copy of such software
22 application;
23 b. installing the software application in a data storage element on a user's computer;
24 c. configuring the software application to require service data to activate at least part of its
25 functionality;
26 d. requiring the user to communicate user data to a remote service system, the user data
27 being derived, at least in part, from identifying data that identifies the user, and being derived, at
28 least in part, from the unique identification code;

1 e. examining user data received by the remote service system to determine whether the user
2 is pirating the software application;

3 f. selectively transmitting service data to the user's computer from said remote service
4 system when said remote service system determines that the user is not pirating the software
5 application; and

6 g. storably receiving the transmitted service data within the data storage element of the
7 user's computer to activate at least part of the functionality of the software.

8
9 36. (New) The method recited by Claim 35 further including the step of archiving user data
10 received from users.

11
12 37. (New) The method recited by Claim 36,

13 wherein received user data for each unique identification code is compared with previously
14 archived user data corresponding to the same unique identification code.

15
16 38. (New) A method of preventing piracy of a given software application comprising the steps of:

17 a. assigning a unique identification code to each authentic copy of such software
18 application;

19 b. installing the software application in a data storage element on a user's computer;

20 c. configuring the software application to require service data, said service data being a
21 necessary component to enable at least part of the functionality of the software application;

22 d. requiring the user to communicate user data to a remote service system, the user data
23 being derived, at least in part, from identifying data that identifies the user, and being derived, at
24 least in part, from the unique identification code;

25 e. examining user data received by the remote service system to determine whether the user
26 is pirating the software application;

1 f. selectively transmitting service data to the user's computer from said remote service
2 system when said remote service system determines that the user is not pirating the software
3 application; and

4 g. storably receiving the transmitted service data within the data storage element of the
5 user's computer to enable at least part of the functionality of the software application.

6
7 39. (New) The method recited by Claim 38 further including the step of archiving user data
8 received from users.

9
10 40. (New) The method recited by Claim 39,
11 wherein received user data for each unique identification code is compared with previously
12 archived user data corresponding to the same unique identification code.